IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Schneider et al.	)	
	)	
Serial No.: 10/600,029	)	Group Art Unit: 2436
	)	
Filed: June 20, 2003	)	Examiner: Mohammad W. Reza
	)	
For: SYSTEM AND METHOD FOR ESTABLISHING AUTHENTICATED WIRELESS CONNECTION BETWEEN MOBILE UNIT AND HOST	)	**Board of Patent Appeals and Interferences**
	)	
Confirmation No.: 6358	)	

Mail Stop: Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF UNDER 37 C.F.R. § 41.41

In response to the Examiner's Answer mailed on January 22, 2009 to the Appeal Brief filed on October 30, 2008 and pursuant to 37 C.F.R. § 41.41, Appellants present this reply brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-29 in the Final Office Action dated July 17, 2008 as clarified in the Advisory Action dated January 22, 2009. The appealed claims are set forth in the attached Claims Appendix.

1. Status of the Claims

Claims 1-29 stand rejected in the July 17, 2008 Final Office Action. Therefore, the final rejection of claims 1-29 is being appealed.

2. Grounds of Rejection to be Reviewed on Appeal

I. Whether claims 1-29 are unpatentable under 35 U.S.C. § 103(a) over U.S. Published Application No. 2003/0172283 to O'Hara (hereinafter "O'Hara") in view of U.S. Patent No. 5,534,857 to Laing et al. (hereinafter "Laing").

3. Argument

In response to the Examiner's Answer, Appellants continue to rely on the arguments made in the Appeal Brief while further distinguishing the claims of the present invention from the prior art in order to reiterate their request that the rejections be reversed on these grounds. In addition, in the Answer, the Examiner has made a number of assertions to which the Appellants wish to respond.

To reiterate, claim 1 recites: "[a] method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of: sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; initiating an authentication process by the second device; *obtaining a PIN code from the user via the DCA,* ***the PIN code identifying at least one device*** *with which the first device is authorized to communicate*; performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes; when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices." (Emphasis added).

In the Examiner's Answer, the Examiner asserts that O'Hara teaches, "obtaining a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate," as recited in claim 1. (See *01/22/2009 Examiner's*

Answer, p. 3, lines 16-22). Specifically, the Examiner indicates that paragraphs [0010] – [0012] and [0021] of O'Hara provide support to his assertion.

Initially, it is respectfully submitted that the Examiner has incorrectly analogized the biometric data of O'Hara to correspond to the PIN code of claim 1. According to the Examiner, "[a]ny ordinary person skill (sic) in art (sic) will agree that the (sic) capturing the personal identification number by a data capturing device and capturing the fingerprint or identity or other indicia as O'Hara's invention teaches are disclosing the same feature of the invention." (See *Id.*, p. 12, line 22 – p. 13, line 3). Appellants strongly disagree with this assertion. The biometric data described throughout the O'Hara reference is neither equivalent to, nor analogous to, the PIN code recited in claim 1.

As opposed to "PIN codes identifying at least one device," it is important to note that data collected in the O'Hara reference is biometric data. (See *O'Hara*, p. 1, ¶ [0010]). The biometric data collected is limited to finger print, voice print, and retinal image (i.e., data having biological characteristics). (See *Id.*, p. 4, ¶ [0039]). The biometric characteristic of this data "*uniquely identifies* ***the user***." (See *Id.*, p. 2, ¶ [0011]). Therefore, the biometric data is limited to identify ***a user*** (i.e., a human being). Clearly, the identification of a human being is separate and distinct from the identification of a device. More specifically, the electronic reading of a particular biological measurable unique characteristic of a human being (i.e., a finger print pattern, a retinal pattern, or a voice pattern) is not remotely comparable to the identification of a device based on a PIN code. Furthermore, the biometric data is limited to only identifying a single human being, since the data is ***unique*** to the user. As recited in claim 1 of the present invention, the PIN code identifies ***at least one device***. The PIN code is not required to be unique to the device, since it may be applied to at least one device (e.g., one or more devices). Thus, multiple devices may have identical PIN codes, according to claim 1, however each piece biometric data is unique to one specific human being.

To further appreciate the distinction between the biometric data and a device identifier, the Examiner needs only to look within the O'Hara disclosure, itself. In fact, O'Hara explicitly teaches ***away*** from the use of "codes" and "PIN numbers" in numerous instances.

For example, O'Hara states:

> Because a biometric characteristic uniquely identifies the user, *there is no need for the user to remember* ***access codes and the like*** in order to define the

functions of the slave device it controls. (See Id., p. 2, ¶ [0011]). (Emphasis added).

O'Hara goes on to state:

> By controlling the functionality of the device 100 using a biometric characteristic such as a finger-print, voice scan, or retinal pattern *there is no need for the device user to remember* ***code words or passwords*** *to enable or disable functionality of the device*, 100 or an appliance that it controls. The biometric characteristics of users can instead be used to uniquely enable or disable features and functions of either the device 100 or its slave. (See Id., p. 2, ¶ [0013]). (Emphasis added).

O'Hara further states:

> By use of the foregoing method and apparatus, readily available biometric sensors can be used to reliably identify a person or persons to whom programming and functionality should be limited or unlimited. *By using biometric characteristics that are unique to an individual, lost or forgotten passwords,* ***PIN numbers****, and keys* ***no longer restrict access to resources***, simplifying security and access to various features. (See *Id.*, p. 4, ¶ [0040]). (Emphasis added).

Therefore, as stated throughout the O'Hara reference, biometric data used to identify a human being eliminates the use of PIN codes. The only evidence the Examiner can provide to support his assertion comes from his statement that "O'Hara, actually disclose (sic) that the device he uses in his invention captures the PIN number and other indicia including identity of the user (See O'Hara, abstract)." (See *01/22/2009 Examiner's Answer*, p. 12, lines 20-22). However, this is simply not true. Upon a careful examination of the Abstract of O'Hara, the Examiner should note the grammatical errors within the portion he is referring to. Specifically, the Abstract states:

> By using biometric characteristics to identify the user, passwords, PIN numbers, keys and other indicia used to establish authorization of a user (sic) enable the authorized user to access programming and subject matter unsuitable for or unintended for unauthorized users. (See O'Hara, Abstract).

It is clear upon reviewing the above-referenced Abstract in conjunction with the Detailed Description of the Preferred Embodiment of the O'Hara reference, particularly ¶ [0040], the Abstract is intended to state that passwords, PIN numbers, keys, and other indicia are no longer needed or used. (See *Id.*, pp. 2-4, ¶¶ [0011]; [0013]; and [0040]). Therefore, the Examiner appears to be hinging his entire argument on a grammatical error within the prior art. Thus, Appellants strongly maintain the position that one of ordinary skill in the art would **not**

agree that obtaining a PIN code to identify at least one device, as recited in claim 1, is the same as collecting a particular biological measurable unique characteristic of a human being, as disclosed in O'Hara.

As detailed above, biometric data is clearly different from PIN codes identifying a device. For the sake of argument, even if the biometric data described in the O'Hara reference is simply considered to be "identification data", this data is still not equivalent to the PIN code recited in claim 1. As emphasized above, the PIN code of claim 1 identifies ***a device***. In its broadest sense, the biometric data (i.e., the finger print) identifies ***a functionality*** of a device. (See *Id.*, pp. 1-5, ¶¶ [0005]; [0010]; [0011]; [0013]; [0022]; [0024]; [0031]; [0040]; and claims 7 and 13). According to O'Hara, the purpose of the biometric identification is to determine whether the user is authorized to access ***a function*** or ***to implement a command*** of a device. The remote control device relies upon biometric characteristics of the user to grant or deny access to certain ***functions and features*** of the controlled slave device "so as to *obviate* the need for passwords or codes." (See *Id.*, p. 2, ¶ [0012]). In other words, the biometric data *prevents* the need for device codes. According to the example provided in O'Hara, a family may want to limit access to television channels having mature subject matter. It is important to make the distinction that O'Hara does not teach or suggest the identification of the television, itself. O'Hara teaches the identification of ***the functionality*** of the television. In contrast to O'Hara, claim 1 states, "the PIN code identifying at least one device with which the first device is authorized to communicate." In other words, the first device can identify which devices it is authorized to communicate with based on the obtained PIN code. Accordingly, different PIN codes may indicate ***different devices***. However, going back to O'Hara, different biometric data indicates the ***same device***. Within this same device, O'Hara provides for ***different functionality*** based on the obtained biometric data. In other words, multiple users, having multiple biometric data is used by the remote control device to communicate with the ***same device***. The data identified by the biometric characteristics does not allow for the remote of O'Hara to distinguish between or identify ***different devices***. In fact, there is no suggestion throughout the O'Hara reference that the remote control device can be in communication with multiple devices at once. Therefore, even if the Examiner argues that O'Hara teaches identification data, it is respectfully submitted that what is being identified is neither analogous to, nor equivalent to, the limitations recited in claim 1. Therefore, O'Hara fails to teach or suggest, "obtaining a PIN code from the

user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate," as recited in claim 1.

It should be noted that the Laing reference was introduced by the Examiner to teach "generating a link key to establish the authenticated wireless communication between the first and second devices," as recited in claim 1. While Appellants do not concede that this limitation is taught by Laing, it is respectfully submitted that Laing does not cure the above-referenced deficiencies of the O'Hara reference. Therefore, for the reasons discussed above and for the reasons previously asserted in the Appeal Brief, Appellants respectfully renew their submission that neither O'Hara nor Laing, either alone or in combination, discloses or suggest "[a] method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of: sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; initiating an authentication process by the second device; *obtaining a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate*; performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes; when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices," as recited in claim 1. (Emphasis added). Thus, it is respectfully submitted that the rejection for claim 1 should be overturned. As claims 2-12 depend from and, therefore, include all the limitations of claim 1, it is respectfully submitted that the rejection for these claims also should be overturned.

Claim 13 recites "[a] system for establishing an authenticated wireless communication, comprising: a first wireless mobile device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; and a second device receiving an initial signal from the first device to establish a wireless communication, the second device initiating an authentication process, *wherein the first device obtains a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate*, wherein the first and second devices perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes, and wherein, when the

pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication." (Emphasis added). Thus, it is respectfully submitted that, at least the reasons discussed above with regard to claim 1, the rejection for claim 13 should be overturned. As claims 14-23 depend from and, therefore, include all the limitations of claim 13, it is respectfully submitted that the rejection for these claims also should be overturned.

Claim 24 recites "[a] wireless mobile device for establishing an authenticated wireless communication with a further device, comprising: a processor; a wireless communication arrangement; and a data capturing arrangement ("DCA") being the only input device interface for a user thereof, wherein the processor generates a request for establishing an authenticated wireless communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device a first sample data, compiled from a collection of random data, and a request for second data, *the DCA obtaining a PIN code from the user, the PIN code identifying at least one device with which the mobile device is authorized to communicate*, the processor generating the second data as a function of the PIN code, the first sample data and the hashing procedure, the second data being provided, by the mobile device, to the further device, wherein the further device generates third data as a function of at least one of the authorized PIN codes stored in a database, the second data received from the mobile device and the hashing procedure, and wherein, when the second data received from the mobile device matches to the third data, the mobile device and the further device generate a link key to establish the authenticated wireless communication." (Emphasis added). Thus, it is respectfully submitted that, at least the reasons discussed above with regard to claim 1, the rejection for claim 24 should be overturned. As claims 25-29 depend from and, therefore, include all the limitations of claim 24, it is respectfully submitted that the rejection for these claims also should be overturned.

4. Conclusion

For the reasons set forth above, Appellants respectfully request that the Board reverse the rejection of the claims by the Examiner under 35 U.S.C. § 103(a), and indicate that claims 1-29 are allowable.

Respectfully submitted,

Date: February 25, 2009

By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276

CLAIMS APPENDIX

1. (Previously Presented) A method for establishing an authenticated wireless communication between a first mobile device and a second device, comprising the steps of:

sending an initial signal by the first device to establish a wireless communication with the second device, the first device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof;

initiating an authentication process by the second device;

obtaining a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate;

performing a pairing process to compare the PIN code to entries in a database of authorized PIN codes;

when the pairing process has been successfully completed, generating a link key to establish the authenticated wireless communication between the first and second devices.

2. (Original) The method according to claim 1, wherein the databases is stored in a memory arrangement of the second device.

3. (Original) The method according to claim 1, wherein the first device is a mobile barcode scanner.

4. (Original) The method according to claim 1, wherein the first device communicates with the second device using Bluetooth technology.

5. (Original) The method according to claim 1, wherein the obtaining step further includes the following substeps:

scanning a barcode using the DCA, the barcode being provided by the user as the PIN code, and

converting the barcode into the PIN code using a processor of the first device.

6. (Original) The method according to claim 1, wherein the second device includes a wireless access point which communicates with the first device.

7. (Original) The method according to claim 1, wherein the first device includes an alerting arrangement notifying the user when to enter the PIN code.

8. (Original) The method according to claim 7, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

9. (Original) The method according to claim 1, wherein the obtaining step includes the following substeps:

limiting a time period for the user to enter the PIN code to a predetermined time period, and

refusing to accept the PIN code from the user when the predetermined time period has expired.

10. (Previously Presented) The method according to claim 1, wherein the pairing process includes the following substeps:

compiling a first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

11. (Original) The method according to claim 1, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

12. (Original) The method according to claim 1, further comprising the step of:
establishing a secure communication between the first and second devices using a predetermined encryption technology.

13. (Previously Presented) A system for establishing an authenticated wireless communication, comprising:

a first wireless mobile device including only a data capturing arrangement ("DCA") as an input device interface with a user thereof; and

a second device receiving an initial signal from the first device to establish a wireless communication, the second device initiating an authentication process,

wherein the first device obtains a PIN code from the user via the DCA, the PIN code identifying at least one device with which the first device is authorized to communicate, wherein the first and second devices perform a pairing process to compare the PIN code to entries in a database of authorized PIN codes, and wherein, when the pairing process has been successfully completed, the first and second devices generate a link key to establish the authenticated wireless communication.

14. (Original) The system according to claim 13, wherein the second device includes a memory arrangement storing the database.

15. (Original) The system according to claim 13, wherein the first device is a mobile barcode scanner.

16. (Original) The system according to claim 13, wherein the first device communicates with the second device using Bluetooth technology.

17. (Original) The system according to claim 13, wherein the first device scans a barcode using the DCA, the barcode being provided by the user as the PIN code, a processor of the first device converting the barcode into the PIN code.

18. (Original) The system according to claim 13, wherein the second device includes a wireless access point which communicates with the first device.

19. (Original) The system according to claim 13, wherein the first device includes an alerting arrangement notifying the user to enter the PIN code.

20. (Original) The system according to claim 19, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a light in a predetermined lighting patterns.

21. (Previously Presented) The system according to claim 13, wherein the pairing process includes the following substeps:

compiling a first sample data, from a collection of random data, by the second device, the second device then providing the first sample data to the first device,

generating second data, by the first device, as a function of the first sample data, the PIN code and a hashing procedure;

providing at least a portion of the second data by the first device to the second device,

generating third data by the second device as a function of at least one of the authorized PIN codes stored in the database, the second data received from the first device and the hashing procedure;

comparing, by the second device, the second data received from the first device to the corresponding third data, and

when the second data received from the first device matches to the third data, generating an indication the pairing process is successfully completed.

22. (Original) The system according to claim 15, wherein the link key is one of a temporary key which is effective only for a single session and a long-term key which is effective for multiple sessions between the first and second devices.

23. (Original) The system according to claim 13, wherein the first and second devices establish a secure communication using a predetermined encryption technology.

24. (Previously Presented) A wireless mobile device for establishing an authenticated wireless communication with a further device, comprising:

a processor;

a wireless communication arrangement; and

a data capturing arrangement ("DCA") being the only input device interface for a user thereof,

wherein the processor generates a request for establishing an authenticated wireless communication, the request being forwarded to the further device via the communication arrangement, the communication arrangement receives from the further device a first sample data, compiled from a collection of random data, and a request for second data, the DCA obtaining a PIN code from the user, the PIN code identifying at least one device with which the mobile device is authorized to communicate, the processor generating the second data as a function of the PIN code, the first sample data and the hashing procedure, the second data being provided, by the mobile device, to the further device,

wherein the further device generates third data as a function of at least one of the authorized PIN codes stored in a database, the second data received from the mobile device and the hashing procedure, and

wherein, when the second data received from the mobile device matches to the third data, the mobile device and the further device generate a link key to establish the authenticated wireless communication.

25. (Previously Presented) The mobile device according to claim 24, wherein the mobile device is a mobile barcode scanner.

26. (Previously Presented) The mobile device according to claim 24, wherein the mobile device communicates with the further device using Bluetooth technology.

27. (Previously Presented) The mobile device according to claim 24, wherein the DCA scans a barcode which is provided by the user as the PIN code, the processor converting the barcode into the PIN code.

28. (Previously Presented) The mobile device according to claim 24, further comprising:
an alerting arrangement notifying the user to enter the PIN code.

29. (Previously Presented) The mobile device according to claim 24, wherein the alerting arrangement includes at least one of a speaker emitting a predetermined sound and a set of LEDs emitting a predetermined lighting pattern.

EVIDENCE APPENDIX

No evidence has been entered or relied upon in the present appeal.

RELATED PROCEEDING APPENDIX

No decisions have been rendered regarding the present appeal or any proceedings related thereto.